Il laboratorio in INTERNET: criteri di affidabilità, sicurezza e qualità

Introduzione: sicurezza come probabilità

Con lo sviluppo dei sistemi informatici di laboratorio, di ospedale e di azienda sanitaria, premuti da utenti e fornitori, stiamo interrogandoci in molte sedi ed a più livelli sulla sicurezza informatica.
Il ventaglio delle posizioni individuali, in parte razionali e in parte emotive, va dalla ricerca della garanzia assoluta, della "blindatura" contro qualsiasi rischio, alla eccessiva banalizzazione del problema.
A pensarci bene, la questione della sicurezza informatica presenta qualche somiglianza con i temi della sicurezza degli operatori contro il rischio di incidenti e malattie, temi sicuramente già noti nei laboratori clinici. Il punto di contatto è costituito dal concetto di "rischio" come "probabilità" e dal rapporto del "rischio" con il beneficio.

Sistemi chiusi e sistemi aperti

L'utilizzo delle tecnologie informatiche avanzate, in particolare della rete INTERNET, è sicuramente ancora rallentato da una vaga percezione di insicurezza da parte di molti. Leggere informazioni di carattere generale è piacevole e utile, mentre scambiare dati personali genera ancora qualche perplessità, anche se si tratta di informazioni comunque a basso rischio di intrusione o alterazione.
L'avanzata delle connessioni di rete, tuttavia, è ineluttabile. Il sistema sanitario nazionale inglese ha accettato da tempo questo concetto e lo sta portando lentamente alle estreme conseguenze, con prudenza ma con determinazione (1). Si stanno diffondendo modelli di "ospedale virtuale" che connettono tra di loro con la telematica non già strutture sanitarie distribuite nel territorio (ospedali, distretti, ambulatori medici), bensì i pazienti stessi con la struttura ospedaliera specialistica (2).
Il sistema tradizionale di conservazione e scambio di informazioni, infatti, è quanto di meno efficiente si potesse escogitare. La maggior parte delle informazioni è ridondante, obsoleta, poco accessibile. La semplice funzione di "deposito" offerta dalla rete INTERNET costituirebbe un progresso rivoluzionario (3).
Il sistema inglese è partito utilizzando reti chiuse dedicate alle strutture sanitarie. Oggi però si dimostra che anche la rete aperta può essere un valido mezzo di comunicazione (4).

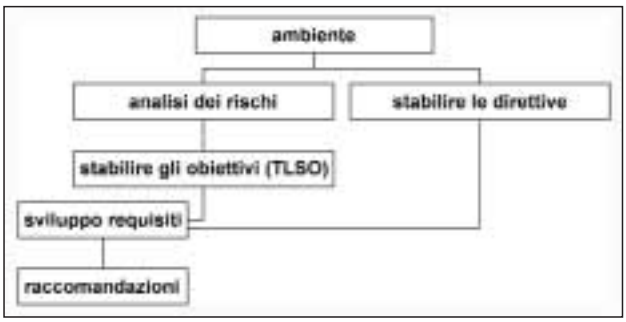
Sicurezza nei sistemi informatici

I laboratori inglesi sono stati coinvolti pesantemente nel progetto telematico (5-7). Hanno individuato e risolto con un sistema originale di consultazione e sviluppo delle idee (*Issues Resolution Mechanism*) più di 50 singole difficoltà, alcune delle quali proprio legate alla sicurezza (8). Ad esempio, il tema numero 35 (*Handling modified or cancelled reports*) è stato risolto stabilendo la presenza di un campo che indicasse la natura di risultato cancellato o modificato (9).
In Europa l'organismo ufficiale di standardizzazione (CEN) (10) si è occupato, tramite un comitato tecnico (TC numero 251) (11) della sicurezza informatica. Vengono da lì alcune importanti distinzioni: affidabilità (= *safety*) come garanzia contro il rischio di arrecare danno, sicurezza (= *security*) come protezione della riservatezza e dell'integrità (12). Viene dal CEN TC 251 inoltre uno standard specificamente dedicato alla sicurezza di un sistema informatico sanitario, identificato dalla sigla CEN ENV 12924, disponibile in Italia attraverso l'UNI (13).

CEN ENV 12924: la valutazione del profilo di rischio

Il messaggio importante del CEN ENV 12924 è che la garanzia di sicurezza non si ottiene con una semplice ricetta, ma al termine di un processo, in cui l'analisi di vari fattori (ambiente, dati, persone, dispositivi) consente di comparare rischi effettivi e benefici attesi e di procedere quindi alla definizione dei requisiti necessari per il sistema (Figura 1).

Figura 1. CEN ENV 12924: processo per garantire sicurezza



I primi passi del processo di classificazione della sicurezza richiedono la valutazione delle caratteristiche di disponibilità, riservatezza ed integrità dei dati (Tabella I). Mediante la risposta a domande specifiche il profilo di sicurezza emerge spontaneamente: disponibilità dei dati critica o non critica; per la riservatezza (= *confidentiality*) dati sensibili, molto sensibili o non sensibili; integrità critica o non critica (Tabella II). Si esaminano quindi l'ambiente fisico, la connessione fisica e la connessione logica del sistema informatico. Ne risultano 6 categorie e altrettanti profili di protezione (Tabella III). A mero titolo di esempio, un PC isolato destinato alla ricerca potrebbe stare nel profilo I, mentre quello di un laboratorio sale al III livello ed una cartella clinica elettronica al VI.

Le caratteristiche ambientali e di connessione

Accessibilità fisica, lontananza dalla sorveglianza, la presenza di personale e la sorveglianza in assenza di pubblico sono elementi che formano il profilo di rischio dal punto di vista fisico ambientale (*Physical Environment Assumption, PEA*).
Il PEA va da 1 a 6 (Tabella IV). La connessione fisica in rete (*Physical Connectivity Assumptions, PCA*) può essere assente, intermittente o permanente (PCA 1, PCA 2 o PCA 3). La connessione logica (*Logical Connectivity Assumptions, LCA*) può essere a dominio singolo, a domini multipli interni, a domini multipli esterni (LCA 1, LCA 2 o LCA 3).

CEN 12924: i profili di protezione

I profili sono composti da requisiti del sistema, requisiti amministrativi, requisiti del personale ed infine requisiti dell'ambiente (Tabella V).
I requisiti di sistema comprendono l'identificazione e l'autenticazione dell'utente, mediante *password*, a cui va aggiunto un dispositivo elettronico di identificazione se il computer si trova in aree con accesso publico (PEA 5 o 6). L'accesso al sistema (*log on*), riuscito o non riuscito, deve essere registrato. L'accesso inattivo (tipicamente per non più di 15 minuti) deve essere interrotto. Il terminale dovrebbe essere sconnesso, con messaggi visivi e sonori, dopo ulteriori 30 minuti di inattività.
Alle categorie superiori (II-VI) corrispondono profili di protezione con requisiti più stringenti (Tabella VI) e poi ulteriori requisiti specifici per i singoli profili sono elencati nel CEN ENV 12924. Ad esempio, nel profilo II la validazione dei dati è fatta da una persona diversa da quella che li ha inseriti. Nel profilo IV la confidenzialità dei dati è protetta mediante crittografia. Al profilo VI troviamo la ridondanza nelle unità di processo, tale da garantire l'assenza di interruzioni del servizio (la disponibilità dei dati è critica nel giro di minuti, non di ore).
Esistono diversi strumenti CEN per la sicurezza informatica, specifici per singoli dispositivi o procedure: ENV 12388 - firma digitale (14), prENV 12251 - password (15), WI 6.4 - PT37 - carte a microprocessori, WI 6.10 - PT 39 - comunicazioni, WI 6.12 - dispositivi a connes-

Tabella I. ENV 12924: Processo di classificazione della sicurezza e specificazione dei requisiti

Passo 1.	Valutare ACI (disponibilità - riservatezza - integrità)
Passo 2.	Individuare la categoria
Passo 3.	Individuare i requisiti di base
Passo 4.	Costruire il profilo di protezione: categoria + requisiti di base + requisiti di livello superiore
Passo 5.	Realizzazione dei requisiti
Passo 6.	Procedere con la sicurezza

Tabella III. Categorie di rischio per la sicurezza informatica

I:	A.nc, Cs, I.n-c
II.	A.nc, Cs, I.c
III:	A.c, Cs, I.c
IV:	A.nc, C.v-s, I.n-c
V:	A.nc, C.v-s, I.c
VI	A.c, C.v-s, I.c

Tabella II. Valutazione di disponibilità, riservatezza, integrità

A = disponibilità	domanda 1: la non disponibilità delle informazioni può causare cattivo o prolungato trattamento? domanda 2: se le informazioni non sono disponibili, ne risultano conseguenze finanziarie, legali o altro? *considerare lo scenario peggiore - non tener conto di copie elettroniche o su carta*
C = riservatezza (confidentiality)	domanda 1: il sistema contiene, elabora o trasmette informazioni personali identificabili? domanda 2: svelare i dati sanitari a estranei può causare imbarazzo o pericolo, diretto o indiretto? domanda 3: svelare i dati sanitari a estranei può dare conseguenze per l'organizzazione sanitaria (danno finanziario, legale, commerciale o imbarazzo della struttura) ? *considerare attentamente i dati anche non identificati direttamente, ma identificabili mediante inferenza* *considerare lo scenario peggiore - non tener conto dei rimedi esistenti*
I = integrità	domanda 1: errori o mancanze possono causare cattivo o prolungato trattamento? domanda 2: in caso di errori o mancanze, risultano conseguenze finanziarie, legali o altro? *considerare lo scenario peggiore - non tener conto di eventuali misure correttive*

Tabella IV. Profilo di rischio fisico ambientale

caratteristica	PEA 1	PEA 2	PEA 3	PEA 4	PEA 5	PEA 6
inaccessibile al pubblico	S	N	N	N	N	N
vicino	S	N				
presenza staff			S	S	N	N
presidiato in assenza pubblico			S	N	S	N

Tabella V. Requisiti del profilo di protezione I per la categoria I

Sistema	Requisiti amministrativi	Requisiti personale	Requisiti fisici e ambientali
• pw (+hw PEA 5-6)	• security manager	• assunzione	• computer principale
• precedente log-on	• security policy	• gestione	• furto
• automatismo log-out	• virus	• addestramento	• elettricità, aria, fuoco, acqua
• privilegi	• manutenzione	• fine rapporto	
• registrazioni etc..	• documentazione		

Tabella VI. Requisiti aggiuntivi per i profili di protezione superiori (II - VI)

Sistema	Requisiti amministrativi	Requisiti personale	Requisiti fisici e ambientali
• identificazione terminali	• quality plan	• idem	• accesso controllato
• registrazione operazioni	• prove sistema separato		• identificazione
• backup affidabile	• verifiche documentate		• orari
• firewalls	• etc..		• area esterna, parcheggio etc..
• etc..			

sione discontinua, WI 6.14 - quadro per le comunicazioni, WI 6.15 - quadro per connessioni intermittenti, FM-HSP/FR - N00-029 - quadro per modelli formali (12).

Conclusioni

Che piaccia o no, le informazioni diagnostiche circoleranno prima o poi in rete aperta per essere là dove servono, nel reparto, nell'ambulatorio, al domicilio del paziente, ovunque. La sicurezza non è un concetto astratto ed assoluto, ma l'espressione di un rischio calcolato con tecniche precise e controllato con misure ben dosate. Il processo per valutare il rischio e realizzare il sistema di sicurezza può essere guidato da norme standard come il CEN ENV 12924.

M. Pradella

Pubblicazioni recensite

CEN Report CR 13694. Health Informatics - Safety and Security Related Software Quality Standards for Healthcare (SSQS). Brussels: CEN 1999

CEN/TC 251/WG III Health informatics - Framework for formal modelling of healthcare security policies. CEN/TC 251/N00-088. Stockholm: 2000

CEN/TC 251/WGIII. Proposal for a work item description for the revision of ENV 12924: Security Categorisation and Protection for Healthcare Information System. CEN/TC 251/N00-082. Stockholm: 2000.

Bibliografia

1. Keen J, Wyatt J. Back to basics on NHS networking. BMJ 2000; 321: 875-8.
2. Jones J. Britain's first "virtual hospital" gets go ahead. BMJ 2000; 320: 1227.
3. Internet based repository of medical records that retains patient confidentiality Roy Schoenberg and Charles Safran BMJ 2000; 321: 1199-203.
4. Using the internet to access confidential patient records: a case study D W Chadwick, P J Crook, A J Young, D M McDowell, T L Dornan, and J P New BMJ 2000; 321: 612-4.
5. http://www.gpnet.nhsia.nhs.uk/pathology/pathology.asp
6. http://www.leeds.ac.uk/acb/pathedi
7. http://www.gpnet.nhsia.nhs.uk/pathology/readme.asp
8. http://www.leeds.ac.uk/acb/irm/
9. http://129.11.239.213/IRM/Queries/IssuesDetail.asp?ID=35
10. http://www.cenorm.be/
11. http://www.centc251.org/
12. CEN Report CR 13694. Health Informatics - Safety and Security Related Software Quality Standards for Healthcare (SSQS). Brussels: CEN 1999.
13. UNI EN 12924 Vategorizzazione della sicurezza e protezione dei sistemi informativi sanitari. EN 12924. Health Informatics - Security Categorisation and Protection for Healthcare Information Systems. Milano: UNI, 1998.
14. CEN EN 12388 Health Informatics - Algorithm for Digital Signature Services in Health Care.
15. CEN EN 12251. Medical Informatics - Secure user identification for healthcare:management and security of passwords - Healthcare oriented IT security funcionality class. Brussels: CEN 1999.